K&L Gates LLP
One Newark Center, Tenth Floor
Newark, New Jersey 07102
Telephone: 973.848.4000
Facsimile: 973.848.4001
Attorneys for Defendant Kenneth Lowson

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA, v. KENNETH LOWSON, a/k/a "Money", KRISTOFER KIRSCH, a/k/a "Robert Woods", JOEL STEVENSON and FAISAL NAHDI.	Hon. Katharine S. Hayden Criminal No. 10-114 (KSH) **MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE SUPERSEDING INDICTMENT** **Filed Electronically**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative History

Other Authorities

K&L Gates LLP
One Newark Center, Tenth Floor
Newark, New Jersey 07102
Telephone: 973.848.4000
Facsimile: 973.848.4001
Attorneys for Defendant Kenneth Lowson

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA, v. KENNETH LOWSON, a/k/a "Money", KRISTOFER KIRSCH, a/k/a "Robert Woods", JOEL STEVENSON and FAISAL NAHDI.	Hon. Katharine S. Hayden Criminal No. 10-114 (KSH) **MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE SUPERSEDING INDICTMENT**

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE SUPERSEDING INDICTMENT

I. INTRODUCTION

> *"The [Computer Fraud and Abuse Act] is a remarkably broad statute … federal prosecutors eventually will try to exploit the breadth and ambiguity of the statute to bring prosecutions based on aggressive readings of the statute."*[1]

The Government's Superseding Indictment (the "Indictment") is a naked effort to punish legal conduct under federal law – the resale of event tickets – by using the Computer Fraud and Abuse Act ("CFAA"), a statute that has nothing to do with so-called "ticket scalping." As this motion to dismiss will illustrate, the Government is trying to "exploit the breadth and ambiguity of the CFAA" by casting alleged breaches of website terms of service as federal crimes, a

[1] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1557 (2010).

strategy that presents this Court with an issue of first impression: Can the CFAA be interpreted to criminalize breaches of contractual terms of service related to online ticket sales? Under the plain language of the statute, related rules of construction, and the United States Constitution, the resounding answer to that question is "no" and dismissal of the unprecedented CFAA-related counts is required.

Hedging its bet on this novel CFAA claim, the Government also alleges wire fraud based upon the same alleged breaches of contract that form the foundation for the CFAA counts. Contrary to the Government's expansive view, 18 U.S.C. § 1343 applies where the alleged victim is actually the target of an attempt to defraud them of "money or property." To overcome the hurdle presented by the limited scope of the wire fraud statute, the Government seeks to expand the well-established definition of "property" to include a seller's right to refuse to sell to particular customers and the related goodwill associated with such an interest. These alleged "interests" are not "property." Dismissal of the wire-fraud counts is required.

II. BACKGROUND

A. Overview of the Indictment

Buried in the Indictment's dizzying array of technical jargon and background puffery, the Government makes the following straightforward and remarkable contention: Defendants have committed federal crimes by allegedly violating online ticket vendors' terms of use, *i.e.*, breaching internet contracts prohibiting the use of automation to purchase event tickets. This allegation is the heart of the Indictment because under two of the three CFAA sections at issue, the Government must establish as an element of the offense that Defendants accessed protected computers "without authorization (or exceeds authorized access)."[2] Although the Indictment

[2] (Indict. at 49, 51).

uses misleading rhetoric in an effort to establish that these alleged breaches of contract were part of a complex conspiracy – purportedly accomplished through a "nationwide web" of computers using "Bots" to make "surreptitious" ticket purchases – the fact remains that this prosecution is grounded upon Defendants' alleged purchase of event tickets on behalf of brokers, for full price from publicly-available websites, in a manner which allegedly breached contractual terms of use. (Indict. at 10).

The Indictment discusses at some length Defendants' alleged "circumvention" of a free technology called "CAPTCHA" by utilizing an automated program that the Government calls the "CAPTCHA Bots." (Indict. at 17, ¶ 10). According to the Government, this alleged "circumvention" of CAPTCHA is significant because the online ticket vendors established contractual "Terms of Service that expressly stated that users were not permitted to access a CAPTCHA-protected website using automated software" – terms of service that the Government candidly admits were necessary "[t]o make clear the purpose of CAPTCHA" to users of the vendors' websites. (Indict. at 9-10, ¶ 1(n)). To illustrate this point, the Government has incorporated an example of a no-automation term of use into the Indictment. (Indict. at 11, fig. 2). Against this backdrop, the Indictment alleges that in the process of purchasing tickets:

> The CAPTCHA Bots would automatically respond to CAPTCHA Challenges on the Online Ticket Vendors' websites and click a box containing a user's acceptance of the Online Ticket Vendors' terms of service, despite the fact that Wiseguys and the CAPTCHA Bots were then violating those same terms of service.

(Indict. p. 23, ¶ 26) (emphasis added).

In effect, the Indictment seeks to convert alleged contractual breaches to virtual breaking and entering. This conversion is supported by inflammatory buzzwords like "circumvention"

and "hacking" in the Indictment,[3] even though the Indictment is clear that the alleged access violation was accomplished via a breach of the terms of service. It is unquestionably true that if the vendors had not adopted terms of use prohibiting automation, it would not have been prohibited at all. The Indictment's hollow "hacking" rhetoric is an attempt to minimize the breathtaking sweep of the actual theory of prosecution.

This case is and has always been about contractual terms of use. At the very inception of this case, the Government's probable cause affidavits for search warrants asserted, "[t]he FBI is conducting an investigation into the use of computer programs, commands and software (collectively "computer programs") designed to subvert the explicit Terms of Use of Ticketmaster," Yankow Affidavit in Support of Warrant at 5, ¶10, Oct. 28, 2008 (emphasis added), and "[t]here is probable cause to believe that the computer programs violate the Terms of Use explicitly set forth by Ticketmaster and permit users to thereby exceed their authorized access to Ticketmaster's computers ..." *Id.* at 5, ¶ 11 (emphasis added).[4]

Indeed, this case is not about computer fraud at all, as is clear from a review of what the Indictment does not allege:

- **The Indictment does not allege that Defendants obtained any information that was restricted from public access.** Instead, the government alleges that Defendants obtained event tickets by paying for them, but accomplished that task by answering CAPTCHA challenges in a manner that allegedly violated the online vendors' terms of service prohibiting the use of automation on their public websites. (Indict. at 23, ¶ 26).

- **The Indictment does not allege that Defendants "broke in" to non-public server locations or web pages.** Instead, the Indictment alleges that Defendants viewed public web sites and provided the same responses to CAPTCHA challenges that any member of the public would have provided to access pages that likewise were available to the general public – except that instead of typing

[3] (Indict. at 15-17).

[4] Defendants have moved to suppress evidence seized pursuant to this and other warrants.

the responses manually, Defendants allegedly used automation in violation of contractual terms of service. (Indict. at 23, ¶ 26).

- **The Indictment does not allege that Defendants stole any property.** Because the tickets were paid for at the full prices asked by the vendors, the Government alleges that Defendants defrauded the vendors out of "valuable property interests," *i.e.*, the right to refuse to sell the tickets to automated purchasers, their goodwill and their "right" to be exclusive distributors. (Indict. at 6, ¶ 2(c)).

- **The Indictment does not allege that Defendants defrauded individual ticket purchasers.** The Indictment does allege that Defendants sold the tickets to brokers who pre-negotiated the prices they would pay for the tickets. (Indict. at 25, ¶ 32).

This Indictment does not seek to punish computer fraud, it inappropriately tries to regulate the legal secondary market for event ticket sales through an overreaching prosecution.

B. The CFAA Counts

The Government alleges violations of the CFAA in counts 2-26 of the Indictment, setting forth three distinct claims. In counts 2-10, the Indictment alleges that Defendants violated 18 U.S.C. § 1030(a)(2)(c), namely that Defendants "intentionally accessed a protected computer"; "without authorization (or exceeded authorized access)"; and "thereby obtained information from any protected computer." (Indict. at 49-50). The Indictment does not specify the "information" Defendants allegedly obtained that is at issue in these counts, because the actual claim is that Defendants obtained tickets. (Indict. at 49-50).

In counts 11-20, the Indictment alleges that Defendants violated 18 U.S.C. § 1030(a)(4), namely that Defendants "accessed a protected computer"; "without authorization (or exceeded authorized access)"; "knowingly and with the intent to defraud"; and "thereby obtained any thing of value." (Indict. at 51-52). The "any thing of value" Defendants allegedly obtained were the tickets, which the Government acknowledges were paid for in full. And the alleged "fraud" is identical to the alleged access violation: The Indictment contends Defendants exceeded

authorized access by purchasing tickets with automation in violation of terms of service, and defrauded the vendors by doing the same thing.

Finally, in counts 21-26, the Indictment alleges that Defendants violated 18 U.S.C. § 1030(a)(5), namely that Defendants "knowingly caused the transmission of a program, information, code or command"; "to a protected computer"; and "intentionally caused damage without authorization." (Indict. at 53-54). The alleged "damage" at issue in these counts – a term the CFAA defines narrowly – is not specified in the Indictment, because there is none.

C. The Wire Fraud Counts

The Government alleges wire fraud in counts 27-43 of the Indictment. The Government's theory of fraud is again the same as its theory of unauthorized access: Defendants allegedly violated terms of service by using automation to purchase tickets even though they agreed to the terms of service stating that they would not use automation. To make this sound like more than a breach of contract, the Government claims that the above process constituted "impersonation" of users.

The Government's theory of the "money or property" allegedly obtained by Defendants is not entirely clear, although Defendants are not accused of obtaining "money" from anyone but brokers, who paid negotiated prices for tickets and allegedly provided the credit cards that were used to purchase them from the vendors. (Indict. at 24-25). And because Defendants paid for the tickets (actually, the brokers paid for the tickets), the Government alleges several alternative theories of "property": (1) the "property" is the vendors' interest in refusing to sell to automated purchasers; (2) the "property" is the vendors' right to be the exclusive distributor of tickets; and/or (3) the "property" is the vendors' business "goodwill" associated with the ability to ensure "fair" access to ticket sales. (Indict. at 6, ¶ 2(c)).

III. ARGUMENT

The failure of an indictment to state an offense under the statute(s) upon which the counts are based is a "fundamental defect" requiring dismissal pursuant to Fed. R. Crim. P. 12(b)(3)(B). *United States v. Spinner*, 180 F.3d 514, 516 (3d Cir. 1999); FED. R. CRIM. P. 12(b)(3)(B). It is not sufficient for an indictment to track the language of the relevant statute(s) in general terms. *United States v. Panarella*, 277 F.3d 678, 685 (3d Cir. 2002) (applying Rule 12(b)(2), predecessor to Rule 12(b)(3)(B)). Instead, the specific facts alleged in the indictment must fall within the scope of the relevant statute(s) as a matter of statutory interpretation or the indictment must be dismissed. *Id.*

A. The Government's breach-of-contract theory of "unauthorized access" must be rejected and counts 2-20 of the Indictment must be dismissed.

In counts 2-20, the Indictment alleges violations of two substantive provisions of the CFAA, both of which require the Government to prove as an element of the offense that the Defendants intentionally accessed a protected computer "without authorization (or exceeds authorized access)." 18 U.S.C. §§ 1030(a)(2)(c) and 1030(a)(4). The Government does not specify whether Defendants' alleged violation was access without authorization, access in a manner that exceeded authorized access, or both.[5]

The truth is that this case has nothing to do with unauthorized access. Websites like ticketmaster.com are publicly available and everyone is authorized to view them. Instead, this

[5] Congress recognized that access violations could be committed by an "outsider" (acting "without authorization") or an "insider," like an employee (who "exceeds authorized access"). Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1630 (2003) [hereinafter *Interpreting Access*] (citing legislative history). Neither scenario contemplated by Congress related to public web pages with contract-based use restrictions, as discussed below.

case is about the Defendants' alleged purchase of tickets, while navigating publicly-available web pages, in a manner that allegedly violated private, contractual terms of use.

As discussed below, the Government's theory that alleged breaches of online terms of use constitute unauthorized access[6] for purposes of a criminal CFAA prosecution fails under the proper, narrow interpretation of the CFAA's language. If the language is ambiguous, the rule of lenity requires that the interpretation favoring Defendants be adopted, and if the Government's interpretation were accepted, the scope of unauthorized access would be unconstitutionally vague.

1. The CFAA prohibits virtual "breaking and entering."

Where the terms of a statute are unambiguous, neither prosecutors nor courts may depart from their plain meaning. *See United States v. Gonzales*, 520 U.S. 1, 8 (1997) (citing *United States v. Wiltberger*, 18 U.S. 76, 95-96 (1820) (Marshall, C.J.) ("Where there is no ambiguity in the words, there is no room for construction. The case must be a strong one indeed, which would justify a court in departing from the plain meaning of words . . . in search of an intention which the words themselves did not suggest")). Criminal statutes like the CFAA must be strictly construed, with any ambiguities resolved in favor of the defendant under the rule of lenity. This approach is necessary because:

> [A] fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear. . . . [and] because of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity.

[6] For convenience, Defendants will refer to "without authorization (or exceeds authorized access)" as "unauthorized access" or as the alleged "access violation" except where relevant distinctions must be drawn.

United States v. Bass, 404 U.S. 336, 347-48 (1971) (all internal quotation marks omitted). Finally, courts should not interpret federal criminal statutes in a way that would substantially alter the balance of power between the federal and state governments, absent a clear directive from Congress. *See United States v. Zwick*, 199 F.3d 672, 683 (3d Cir. 1999), *abrogated on other grounds by Sabri v. United States*, 541 U.S. 600 (2004)).

The CFAA does not define the terms "access" or "without authorization," but does define the phrase "exceeds authorized access" as follows: "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The plain language of these words reflects a prohibition on virtual breaking and entering, not violations of contract-based use restrictions for a public website.[7]

Legislative history supports this common-sense interpretation: "[S]ection 1030 deals with an 'unauthorized access' concept of computer fraud … the conduct prohibited is analogous to that of 'breaking and entering' …" H.R. REP. NO. 98-894 at 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706. Although Congress has streamlined the statute's unauthorized access language, it has never indicated any intention to define unauthorized access based upon the private terms of use established for a public website. In fact, as one commentator has noted, when the CFAA was passed there were no publicly-available computers or websites – the internet had not yet been developed – and so Congress could not have contemplated that

[7] Defendants acknowledge commentators have argued the words do not have a readily ascertainable "plain" meaning. *See* Kerr, *Interpreting Access*, *supra*, at 1621 (citing cases). To the extent that is true, the rule of lenity requires that a narrow interpretation be adopted.

unauthorized access would be defined to include violations of internet terms of use.[8] Rather, Congress clearly intended to criminalize theft of private information that had been secured by the owner in a manner analogous to locking a door or a safe. The Government's theory that contractual terms of use can establish criminal access restrictions for public websites is contrary to the statute's plain language and congressional intent. *See, e.g., United States v. Nosal*, No. C 08-0237 MHP, 2010 WL 934257, at *6 (N.D. Cal. Jan. 6, 2010) "[t]here is simply no way to read that definition [of "exceeds authorized access"] to incorporate corporate policies governing use of information … [s]uch an interpretation would defy the plain meaning of alter, as well as common sense.") (emphasis added).

2. A contract-based interpretation of unauthorized access would run afoul of the vagueness doctrine.

There has never been a successful criminal CFAA prosecution based on the violation of a public website's terms of service. There has, however, been a failed one – *United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009). In *Drew*, the court held that if the CFAA is interpreted to criminalize internet terms of use, it is unconstitutionally vague. *Id.*[9]*; see also*

---

[8] Nicolas R. Johnson, *"I Agree" to Criminal Liability: Lori Drew's Prosecution Under § 1030(A)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561, 567 (2009).

[9] In *Drew*, the defendant registered and created a profile for a fictitious 16 year old male named "Josh Evans" on www.myspace.com ("MySpace") in violation of MySpace's terms of service and used this profile to commit a tort (intentional infliction of emotional distress) against a 13 year old girl named Megan Meier ("Megan"). *Drew*, 259 F.R.D. at 464. The defendant, posing as Josh Evans, contacted and flirted with Megan over the course of several days, but eventually informed Megan that "Josh" was moving away and that he no longer liked Megan, even telling her that "the world would be a better place without her in it." *Id.* Later that same day, Megan, who had a history of mental health issues, committed suicide. *Id.* The defendant was convicted of a misdemeanor violation of Section 1030(a)(2)(C) of the CFAA. *Id.* The defendant then filed a motion for judgment of acquittal, alleging the evidence was insufficient to support a conviction. *Id.* at 455-56. On review, the court held that construing the terms of service as establishing the scope of authorized access under the CFAA violated the void-for-vagueness doctrine. *Id.* at 462, 464.

Nosal, 2010 WL 934257, at *6 (unauthorized access cannot be based on "corporate policies governing use of information").

The constitutional vagueness doctrine has three components – (i) it bars enforcement of "a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application"; (ii) the previously-discussed "rule of lenity ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered"; and (iii) "due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *United States v. Lanier*, 520 U.S. 259, 266 (1997) (all internal citations and quotation marks omitted). The touchstone of these three components is whether the statute, as applied, makes it "reasonably clear at the relevant time that the defendant's conduct was criminal." *Id.* at 266-67. The *Drew* court's analysis provides a useful framework to consider the vagueness problems raised by the Government's contract-based theory of prosecution in this case.

First, the court in *Drew* held that an individual of "common intelligence" would not be on notice that a breach of terms of service could be a federal crime. *See* 259 F.R.D. at 464. The court reasoned that "[n]ormally, breaches of contract are not the subject of criminal prosecution," and that the language of the CFAA does not explicitly state that the "CFAA has 'criminalized breaches of contract' in the context of a website terms of service." *Id.*

This reasoning makes sense and safeguards against absurd results. For example, most people likely do not know that in many states, a 17 year-old boy who runs a Google search for a

school project has agreed to Google's terms of service by "using the services."[10] Having agreed to the terms, the 17 year-old also has violated Google's terms of service, which state "[y]ou may not use the Services and may not accept the Terms if … you are not of legal age to form a binding contract with Google."[11] Under the Government's contract-based definition of unauthorized access, this 17 year-old has committed at least a federal misdemeanor.[12] If the student typed "legal age to enter a contract" into Google's search engine, his violation would at least be ironic.[13]

Second, the court in *Drew* also reasoned that the contract theory of unauthorized access injected an impermissible level of indefiniteness into the analysis. *Id.* For example, the court pointed out that the MySpace terms of service contained an arbitration clause, and it was unclear whether a finding of unauthorized access could be made without arbitration. *Id.* This is not a trivial point – if proving a breach of contract is required to establish an element of a criminal CFAA offense, then adjudication of contract-based defenses (potentially in forums specified in

---

[10] Google Terms of Service, Section 2.2(B), http://www.google.com/accounts/TOS (last visited on June 25, 2010).

[11] *Id.* at Section 2.3.

[12] 18 U.S.C. § 1030(a)(2)(c) requires only access without authorization, and the acquisition of "information." Since the point of a Google search is to get information, the 17 year-old is out of luck.

[13] Running that search on Google yields a "Wiki Answers" result as the first "hit," which states that in the majority of jurisdictions, 18 is the age when a person can validly enter into a contract. *See* Wiki Answers, http://wiki.answers.com/Q/At_what_age_can_one_enter_into_a_legal_contract (last visited on June 25, 2010).

the contracts) is unavoidable, and mini-trials on breaches of contract would be required to establish criminal liability.[14]

Finally, the court in *Drew* held that treating a violation of a website's terms of service as sufficient to constitute a criminal access violation would fail to provide minimal guidelines to govern law enforcement, *Id.* at 466, a point illustrated by the hypothetical 17 year-old Google user discussed above. If every breach of a term of use qualified for prosecution, then there would be "absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution." *Id.* at 467. The court warned that in this situation, "federal law enforcement entities would be improperly free 'to pursue their personal predilections.'" *Id.* (citing *Kolender v. Lawson*, 461 U.S. 352, 357-58 (1983)).

This last point is easily illustrated by reviewing Ticketmaster's terms of use – Ticketmaster prohibits persons younger than 13 from using its website. If a 12 year-old buys a ticket from Ticketmaster.com, they have violated Ticketmaster's Terms of Use. Will the Government prosecute? Perhaps only if the 12 year-old resells the ticket? Indeed, the scope of the Government's prosecutorial authority under a contract-based interpretation of the CFAA would be limited only by the creativity that private parties can employ in drafting – and typically with unilateral authority, revising – their online terms of use. It is not a meaningful response to this problem that the Government is unlikely to abuse that discretion.

The result in *Drew* is consistent with other recent, well-reasoned decisions that have rejected an expansive interpretation of what constitutes unauthorized access for purposes of criminal CFAA liability. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009)

---

[14] Ticketmaster's terms of service contain an arbitration clause. Ticketmaster Terms of Use, ¶ 24, http://www.ticketmaster.com/h/terms.html?tm_link=tm_homeA_i_terms (last visited June 25, 2010).

(applying the rule of lenity and holding that criminal CFAA liability cannot turn on whether the defendant breached a state law duty of loyalty to an employer); *Nosal*, 2010 WL 934257, at *7 ("[T]o the extent that the superseding indictment alleges that [the defendants] exceeded their authorization to access [their employer's] system by violating [the employer's] confidentiality and terms of use agreements, the superseding indictment would also fail to state a violation of section 1030(a)(4)."); *Brett Senior & Assocs., P.C. v. Fitzgerald*, No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007) ("It is unlikely that Congress, given its concern 'about the appropriate scope of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract."); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005) (holding that even if the defendant breached a contract, that breach of a promise not to use information stored on union computers in a certain way did not mean her access was unauthorized). The approach taken by these courts is necessary and wise, because the CFAA's reach is otherwise practically limitless – the statute applies to every computer that is within the scope of authority granted by commerce clause jurisprudence – and as a result, the interpretation given by courts to the terms "access" and "without authorization" has critical significance.[15] To avoid a statute that has no limits at all, these terms must be construed narrowly.[16]

In order to save an otherwise impermissibly vague statute, courts should apply a limiting construction if possible. *See Boos v. Barry*, 485 U.S. 312, 331 (1988) ("We have … instructed 'the federal courts … to avoid constitutional difficulties by [adopting a limiting interpretation] if such a construction is fairly possible."). Within the last month, the United States Supreme Court

---

15 Kerr, *Vagueness Challenges, supra*, at 1575.

16 *Id.*

has affirmed and applied this approach to the construction of broadly-framed criminal statutes. *See Skilling v. United States*, No. 08-1394, 2010 WL 2518587, at *26-30 (June 24, 2010) (construing the "honest services" mail/wire fraud statute as covering only bribery and kickback schemes, in order to prevent the statute from being unconstitutionally vague). This Court should follow the Supreme Court's example and reject the Government's expansive – and unconstitutionally vague – interpretation of the CFAA.

a. *Poorly reasoned civil decisions cannot save the Indictment.*

It is true that several courts have concluded without analysis, in the context of civil CFAA claims, that term of service violations can establish unauthorized access. For example, in *America Online, Inc. v. LCGM, Inc.*, the plaintiff complained that defendants sent large numbers of unauthorized and unsolicited bulk e-mail advertisements to its members in direct violation of its terms of service. 46 F. Supp. 2d 444, 446 (E.D. Va. 1998), . In a one sentence conclusory holding, the court declared that "[d]efendants' actions violated AOL's Terms of Service, and as such was unauthorized" under the CFAA. *Id.* In a factually similar case involving the same plaintiff, the court summarily declared that the limited evidence presented at trial was enough to support the court's preliminary conclusion that "[the defendants] 'exceed[ed] authorized access' by violating the Terms of Service." *America Online, Inc. v. Nat'l Health Care Discount, Inc.*, 174 F. Supp. 2d 890, 899 (N.D. Iowa 2001) (citing *LCGM*, 46 F. Supp. 2d at 446). Neither court analyzed the statute's language, considered issues of due process, vagueness or the rule of lenity, or offered any other analysis of any substance in arriving at that holding.

Other decisions have implied that contracts can define the scope of unauthorized access without analyzing the question *See, e.g., EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003) (observing in dicta that "a lack of authorization could be established by an explicit statement on the website."); *Craigslist, Inc. v. Naturemarket, Inc.*, No. C 08-5065 PJH,

2010 WL 807446, at *12 (N.D. Cal. Mar 5, 2010) (evaluating a recommendation from a magistrate judge regarding the plaintiff's uncontested motion for default judgment and stating, without support, that plaintiffs had sufficiently pled CFAA claim where complaint alleged defendant accessed plaintiff's computers in violation of terms of use); *eBay, Inc. v. Digital point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (citing only *LCGM* and finding defendants access was unauthorized because it violated eBay's terms of use); *Southwest Airlines v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439-40 (N.D. Tex. 2004) (finding that Southwest sufficiently stated CFAA claim where Southwest had directly informed the defendant that its use was unauthorized); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000) (finding that plaintiff successfully established defendant's use of its website was unauthorized simply because the plaintiff objected to defendant's use).

Each decision in this line of cases failed to consider, let alone analyze, the rules of construction that apply to criminal statutes (most notably, the rule of lenity). Nor did these courts, presented with civil claims, express any concern for or appreciation of the consequences of attaching federal criminal liability to internet contract law and the potential that their decisions would support such a result. As the court in *Brett Senior* noted, it is unlikely Congress intended to criminalize breaches of contract. 2007 WL 2043377, at *4. These decisions reflect a failure to appreciate the consequences of giving a criminal statute an expansive interpretation in the context of civil claims, and have been rightly criticized by numerous commentators for that reason. *See Southwest Airlines Co. v. BoardFirst, LLC*, No. 3:06-CV-0891-B, 2007 WL 4823761, at *13 (N.D. Tex. Sept. 12, 2007) (citing Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 368 (2004) (arguing that the CFAA was

designed to prevent computer hacking and "was never intended to afford website owners with a method for obtaining absolute control over access to and use of information they have chosen to post on their publicly available Internet sites."); Kerr, *Interpreting Access, supra*, at 1649; Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 528 (2003) ("An even more serious problem is the judicial application of the [CFAA]…to make it illegal…to seek information from a publicly available website if doing so would violate the terms of a 'browserwrap' license.")). Taking note of these significant criticisms, one court declined to apply its own precedent that a computer use which violates the terms of a contract is unauthorized access. *See BoardFirst*, 2007 WL 4823761, at *13.

B. Counts 2-10 of the Indictment must be dismissed because the Indictment fails to allege that Defendants' obtained "information."

The Indictment utterly fails to identify any alleged "information" that Defendants "obtained" in violation of section 1030(a)(2)(c), thus obfuscating the nature of the felony offense charged in counts 2-10 of the Indictment. Instead, counts 2-10 allege that Defendants obtained tickets, not "information." (Indict. at 49-50). It should go without saying that "tickets" are not "information," but because counts 2-10 identify tickets and not information, Defendants are constrained to say it; the result is that dismissal is required. The Indictment can not and does not allege any facts that would establish that Defendants obtained any "information" other than what is available to every other member of the public that uses the online vendors' public websites.

The Government's position may be – although the Indictment is cryptic – that the CFAA criminalizes the viewing of publicly-available information, so long as the information is viewed in a manner that violates terms of use. Consider as an example the 17 year-old Google user, discussed above, who obtains "information" through an "unauthorized" Google search by violating Google's terms of use. This "Googler" wanted to find out whether he is old enough to

enter into a contract (unfortunately for him under the Government's view of the CFAA, he "obtains information" that both shows he is not old enough, and establishes his criminal culpability at the same time, and so he must rely on the Government's beneficence to avoid at least a misdemeanor prosecution). Indeed, the Government's contract-based theory of unauthorized access logically entails the absurd position that Defendants can be criminally prosecuted – and put in prison, if convicted – for "obtaining" nothing more than publicly-available information. This is true because if a user can commit an access violation under the CFAA by breaching a contract, it will not necessarily be true that the information she "obtains" was restricted from public view – millions of websites contain both publicly-available information and contractual terms of use that routinely are breached. If violating internet terms of use while obtaining publicly-available information is a CFAA violation (as a consistent application of the Government's theory requires), then the universe of federal criminals has been increased exponentially, a result Congress almost certainly did not intend. Given that such a result was not intended, makes no sense, and would result in a massive expansion of federal authority over everyday internet activity, it should be rejected.

C. Counts 11-20 of the Indictment must be dismissed because the Indictment conflates the alleged "fraud" with the alleged "unauthorized access."

The Government's Indictment fails to allege any computer fraud other than the alleged unauthorized access, and accordingly Counts 11-20, alleging violations of section 1030(a)(4), must be dismissed for that additional reason. The Government seeks to prove these separate elements of the offense through precisely the same set of alleged facts, something it may not do. As one trial court explained in the context of a civil CFAA claim:

> [A] section 1030(a)(4) claim … requires both unlawful access and an intent to defraud. In looking to an offender's motivation in accessing information in determining whether the unlawful access requirement has been met, the plaintiff seeks to collapse these independent requirements into a single inquiry: whether the offender intended to use

> impermissibly the information obtained. The plaintiff's interpretation thus runs afoul of the general rule that if possible, courts should adopt constructions that recognize each element of a statute.

Brett Senior, 2007 WL 2043377, at *4 (citing *Ki Se Lee v. Ashcroft*, 368 F.3d 218, 223 (3d Cir. 2004) ("We start with the principle that if at all possible, we should adopt a construction which recognizes each element of the statute.") (emphasis added)); *see also Nosal*, 2010 WL 934257, at *6 ("intent and authorization are independent elements of the CFAA. In other words, an individual's intent in accessing a computer, be it to defraud or otherwise, is irrelevant in determining whether an individual has permission or is authorized to access the computer.") (emphasis added).

The Indictment alleges that Defendants committed an access violation by using automation, in violation of terms of service, to purchase event tickets (Indict. at 16-17), and that Defendants defrauded the online vendors by using automation, in violation of terms of service, to purchase event tickets. (Indict. at 23, ¶ 26). Therefore, the alleged fraud and the alleged access violation are the same thing: The "fraud" ostensibly was committed when one computer program (CAPTCHA Bots) allegedly "deceived" another computer program (Ticketmaster's ticket purchasing web page) by clicking a box indicating acceptance of terms of use even though those terms of use were then being violated. (Indict. at 23, ¶26). This "fraud" is precisely the same automated process the Government contends proves that Defendants committed an access violation. Under the Government's approach, the CFAA's unauthorized access element and fraud element have been conflated into a single inquiry, and dismissal is required.

D. Counts 21-26 of the Indictment must be dismissed because the Government has failed to allege "damage" as that term is defined by the CFAA.

Throwing spaghetti at the wall to see what might stick, the Indictment makes the false and fanciful allegation that Defendants "knowingly transmitted programs, information, code and

commands" – specifically "responses to CAPTCHA Challenges" and "automated ticket purchase requests" – that caused unidentified "damage" to Ticketmaster's computers. (Indict. at 53-54). However, the CFAA defines "damage" narrowly as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Given that "damage" is a defined term, the Indictment must state clearly, in a straightforward manner, what constitutes the alleged "damage." The Indictment's failure to do that is a fatal error.

Instead, the Indictment does not offer even a hint as to how responding to CAPTCHA challenges – conduct that every single user of Ticketmaster's website engages in when they review available tickets – could have caused "damage." Counts 21-26 of the Indictment simply make no effort, even in passing, to identify the alleged "damage" that was caused. The Government instead has opted for misdirection – and in a bizarre *non sequitor,* counts 21-26 identify an "approximate number of users impersonated" with respect to particular events. (Indict. at 53-54). The Indictment does not explain how Ticketmaster's computers were impacted differently by "impersonated users" than by "real users," nor could it since any such claim would be nonsensical.[17] The failure to disclose the alleged damage at issue warrants dismissal of these counts.

E. Counts 27-43 of the Indictment must be dismissed because the Government has alleged a theory of "property" that falls outside the scope of the wire fraud statute.

In counts 27-43, the Indictment alleges wire fraud claims based upon the same factual assertions at issue in the rest of the Indictment – the Defendants' alleged violation of terms of

[17] In fact, the Government's "impersonated users" rhetoric is utter nonsense. Allegedly, actual credit cards owned by actual people were used by other actual people to purchase actual tickets, in an allegedly automated process that violated terms of use. (Indict. at 21-22). At most, these allegations amount to a claim that terms of service were violated, not that users were "impersonated," any more than a man would "impersonate" his wife if she gave him permission to use her credit card to buy a ticket from one of the online vendors.

use in ticket purchasing. To prove mail or wire fraud, the evidence must establish beyond a reasonable doubt (1) the defendant's knowing and willful participation in a scheme or artifice to defraud, (2) with the specific intent to defraud, and (3) the use of the mails or interstate wire communications in furtherance of the scheme. *United States v. Antico*, 275 F.3d 245, 261 (3d Cir. 2001). Additionally, the object of the alleged scheme or artifice to defraud must be a traditionally recognized property right. *United States v. Henry*, 29 F.3d 112, 115 (3d Cir. 1994).

1. The wire fraud statute does not apply to "interests," it applies to "money or property."

The Government has identified three alleged "property interests" that are the object of the alleged wire fraud: (1) the vendors' goodwill; (2) the vendors' right to be exclusive distributors; and (3) the vendors right to define the terms of ticket sales. (Indict. at 6, ¶2(c)). None of these "interests" are property under Third Circuit law for purposes of a wire fraud prosecution.[18]

The Third Circuit has explained that similar "rights" are not "property" under the federal mail and wire fraud statute. *Henry*, 29 F.3d at 115. In *Henry*, the court held that certain banks' right to have a fair opportunity to bid to be the depositories for toll revenues did not constitute "property" that could sustain wire fraud claims arising out of an alleged bid-rigging scheme. *Id.* As the court explained:

> The competing banks' interest in a fair bidding opportunity does not meet this test [of whether the interest is a traditionally recognized property right]. Clearly, each bidding bank's chance of receiving property-the deposits if its bid were accepted-was, at least in part, dependent on the condition that the bidding process would be fair. This condition, which is all that the bidding banks allegedly lost, was thus valuable to them, but it is not a traditionally recognized, enforceable property right…

[18] The Government makes these claims because as noted, the tickets were paid for at full price and because Defendants are not accused of having actually obtained tickets – as the indictment makes clear, Defendants are accused of using brokers' credit cards to purchase tickets for brokers.

> …[o]ur determination that the fair opportunity to bid is not a property right of the competing banks seals the fate of this indictment. It is irrelevant that, as the government points out, the scheme allegedly afforded its participants tangible benefits-over $34,000,000 in deposits for Bank A, and favorable loan treatment and campaign contributions to his political allies for [defendant].

Id. at 115-116. Other courts have followed the same reasoning, including the District Court of New Jersey. *See United States v. Bruchhausen*, 977 F.2d 464 (9th Cir. 1992); *United States v. Alkaabi*, 223 F. Supp. 2d. 583 (D.N.J. 2002). For example, in *Bruchhausen*, the defendant, a German citizen, concocted a plan to smuggle American technology into the Soviet Bloc. 977 F.2d at 466. To effectuate his plan, the defendant deceived manufacturers into selling him products by assuring them that all of the equipment sold would be used only in the United States. *Id.* After the sale, the products were eventually shipped to West Germany and then on to the Soviet Bloc. However, despite his deception concerning the eventual destination of the products, the defendant always paid in full for the merchandise. *Id.*

As a result of his actions, the defendant was convicted on fifteen counts of wire fraud. *Id.* at 466-67. On appeal, the defendant claimed that the wire fraud indictment was insufficient as a matter of law. *Id.* at 467. The court held that a manufacturer's intangible interest in the destination of its products after the sale was not a cognizable property interest within the meaning of the statute. *Id* at 468.

Addressing a theory very similar to the Government's view in this case, the court noted that "[w]hile they may have been deceived into entering sales that they had the right to refuse, their actual loss was in control over the destination of their products after sale. It is difficult to discern why they had a property right to such post-sale control." *Id.* In coming to this conclusion, the court also rejected the government's claim that "the manufacturers lost part of their bargain because they would not have sold the products if they had been told that the products were destined for the Soviet Bloc." *Id.* at 467-68. The court definitively held that

"[t]here is no…understanding that a manufacturer has a property interest in the destination of its products." *Id.* at 468 (emphasis added).

It is also important to note that the court's decision was influenced by the rule of lenity. *Id.* The court observed that the wire fraud statute provided no guidance in determining whether these intangible rights were covered property interests. *Id.*

Similarly, in *Alkaabi*, this Court held that a testing service's interest in maintaining the integrity of its testing process was not "property," and explained:

> [L]ike the integrity of the bidding process in *Henry*, the integrity of the testing process alleged in these cases is not a property right encompassed by the mail fraud statute. The Indictments against Alkaabi and Alsugair join the ranks of other federal cases in which Indictments were dismissed for failure to allege the deprivation of a legally recognized traditional property interest as an element of the mail and wire fraud statutes.

223 F. Supp. 2d at 590-91 (citing *Monterey Plaza Hotel Ltd. P'ship v. Local 483 of Hotel Employees, Rest. Employees Union, AFL-CIO*, 215 F.3d 923, 926 (9th Cir.2000) (dismissing mail and wire fraud charges based on damage to goodwill); *United States v. Walters*, 997 F.2d 1219, 1224-27 (7th Cir.1993) (dismissing mail fraud charge based on university's loss of scholarship money); *Lancaster Cmty. Hosp. v. Antelope Valley Hosp. Dist.*, 940 F.2d 397, 406 (9th Cir.1991) (dismissing mail fraud charge based on loss of market share); *United States v. Zauber*, 857 F.2d 137, 147 (3d Cir. 1988) (dismissing mail and wire fraud charges based on loss of control over spending of pension funds); *Roitman v. New York City Transit Auth.*, 704 F. Supp. 346, 348-49 (E.D.N.Y.1989) (dismissing mail fraud claims based on damage to reputation, good name, honor and integrity)).

The rejection of an expansive view of "property" under the wire fraud statute carries even greater weight in light of a proposed Congressional amendment to the mail and wire fraud statutes that would expand the language beyond money and property, to encompass "any thing of value." *See* 2009 CONG US HR 1825, Sec. 2, "Application of Mail and Wire Fraud Statutes to

Licenses and Other Intangible Rights," (March 31, 2009).

Put simply, Congress has not criminalized the resale of tickets or the use of automation in ticket purchasing. Both are topics that legislatures at the state and federal level can address and in some instances, have addressed or are in the process of addressing.[19] The Government in this case is the tail trying to wag the dog – this indictment is a transparent effort to punish conduct that has not been regulated by Congress. As the Court in *Alkaabi* rightly emphasized:

> As the Supreme Court has explained: "In deciding what is property under § 1341 ... 'it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.'" *Cleveland,* 531 U.S. at 25. This approach is also consistent with the principles of federalism, articulated by the Supreme Court in *Cleveland:* "unless Congress conveys its purpose clearly, it will not be deemed to have significantly changed the federal-state balance in the prosecution of crimes." *Id.* (quoting *Jones v. United States*, 529 U.S. 848, 858 (2000)). Indeed, if Congress wishes to make cheating on tests" a federal crime, it must do so with greater clarity.

223 F. Supp. 2d at 591.

The result in this case should be no different – if Congress wishes to make automated ticket purchasing a federal crime, it must do so with greater clarity. Because it has not, the Government's creative Indictment – two words that should not go together – must be dismissed.

IV. CONCLUSION

For all of the foregoing reasons, Defendants respectfully ask this Court to enter an Order, in the form of the proposed Order attached hereto, dismissing all counts in the Superseding Indictment.

---

[19] Recently, the Vermont legislature passed a law forbidding the use of automated software to purchase tickets from online ticket venders. *See* 9 V.S.A. § 4190(a) ("A person shall not intentionally use a computer program or other software intended to interfere with or circumvent, on a ticket seller's website, an equitable ticket buying process…"). Such a law would be wholly unnecessary if the CFAA was intended to cover this conduct.

Dated: July 2, 2010

Respectfully submitted,

/s/Mark A. Rush
Mark A. Rush, Esquire
Admitted Pro Hac Vice
Andrew R. Stanton, Esquire
Admitted Pro Hac Vice
K&L GATES LLP
K&L Gates Center
210 Sixth Avenue
Pittsburgh, PA 15222-2613
Telephone: 412.355.6500
Facsimile: 412.355.6501

David S. Kwon, Esq.
K&L GATES LLP
One Newark Center, Tenth Floor
Newark, NJ 07102
Telephone: 973.848.4000
Facsimile: 973.848.4001

Attorneys for Defendant Kenneth Lowson

/s/John H. Yauch
Richard Coughlin, Esq.
Federal Public Defender
John H. Youch, Esquire
Assistant Federal Public Defender
1002 Broad Street
Newark, NJ 07102
Telephone: 973.645.6347
Facsimile: 973.645.3101

Attorneys for Defendant Joel Stevenson

/s/John P. McDonald
John P. McDonald, Esq.
McDonald & Rogers, LLC
181 West High Street
Somerville, NJ 08876
Telephone: 908.722.4100
Facsimile: 908.722.7532

Attorneys for Defendant Kristofer Kirsch

CERTIFICATE OF SERVICE

I hereby certify that on the 2nd day of July 2010, a true and correct copy of MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE INDICTMENT was served by electronic filing upon:

Seth B. Kosto, Esq.
Assistant United States Attorney
United States Attorney's Office
970 Broad Street
Suite 700
Newark, NJ 07102

Erez Liebermann, Esq.
Assistant United States Attorney
United States Attorney's Office
970 Broad Street
Suite 700
Newark, NJ 07102

/s/Mark A. Rush, Esq.
Mark A. Rush, Esq.